Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Burgundy Asset Management Ltd. (Organization)
Decision number (file number)	P2020-ND-155 (File #016255)
Date notice received by OIPC	June 18, 2020
Date Organization last provided information	June 18, 2020
Date of decision	November 20, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • telephone number, • date of birth, • email address, • bank information, • social insurance number, • copy of personal identification document, and • signature specimen. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or about April 21, 2020, an employee of the Organization clicked on a phishing email and entered his log-in credentials for his work email account. • Intermittently between April 21, 2020 and May 12, 2020, the credentials were used by an unauthorized party to log into the employee's work email account via the Organization's web-based access. • On May 12, 2020, phishing emails that appeared to spoof the employee's email address were sent to individuals whose information was stored in the employee's email address book.
Affected individuals	The incident affected six (6) Alberta residents.
Steps taken to reduce risk of harm to individuals	• Provided credit monitoring services to affected individuals. • Notified the custodian of the Organization's pooled funds, to red-flag and take extra caution for transactions from affected individuals. • Added alerts to the Organization's CRM system for all affected individuals. • Disabled the Organization's web-based email access. • Reset all employees' access passwords. • Placed an internal red-flag on all impacted clients. • Completed regular and annual security awareness training for all employees, including how to identify a phishing attempt. • Engaged third party cybersecurity consultant to review its security practices. • Reviewing an encryption tool ad spam filter tool. • Conducting a review of policies, procedures and controls to identify and addresses any necessary updates. • Will run an email clean-up campaign to enforce deletion and proper storage of emails.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and follow-up letter or email between May 20, 2020 and June 12, 2020.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization identified "possible financial loss" and "possible identity theft" as harms that might be caused to affected individuals as a result of the incident. In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported, *Although our forensic investigator cannot definitively confirm the personal information has been accessed, we cannot rule out the possibility of information being downloaded or viewed.* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (phishing). Further, it appears the email account was exposed for approximately twenty-two (22) days.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.

A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (phishing). Further, it appears the email account was exposed for approximately twenty-two (22) days.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by telephone, email and letter between May 20, 2020 and June 12, 2020, in accordance with the Regulations. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner